Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A computing apparatus comprising:

a trusted hardware module;

a plurality of further hardware modules;

a shared communication infrastructure by which the hardware modules can communicate with each other; and

a first communication path, distinct from the shared communication infrastructure, by which a first one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

2. (Previously Presented) An apparatus as claimed in claim 1, wherein the trusted hardware module and the first further hardware module each include a respective computing engine which partakes in the direct communication via the first communication path.

3. (Previously Presented) An apparatus as claimed in claim 2, wherein:

the first further hardware module is operable to supply to the trusted hardware module a request for operation on data; and

in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first further hardware module via the first communication path and not via the shared communication infrastructure.

4. (Previously Presented) An apparatus as claimed in claim 3, wherein the trusted hardware module includes means for storing policy information regarding such operations which can or cannot be permitted, and is operable to generate the response with reference to the policy information.

5. (Previously Presented) An apparatus as claimed in claim 1, wherein the trusted hardware module is operable to generate an encryption and/or decryption key and to supply that key to the first further hardware module via the first communication path and not via the shared communication infrastructure.

6. (Previously Presented) An apparatus as claimed in claim 5, wherein the first further hardware module is operable to use the key for encryption and/or decryption of data communicated via the shared communication infrastructure.

7. (Previously Presented) An apparatus as claimed in claim 1, wherein the trusted hardware module is operable to generate a challenge and to supply the challenge to the first further hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path.

8. (Previously Presented) An apparatus as claimed in claim 7, wherein:

in response to the challenge, the first further hardware module is operable to generate a response and to supply the response to the trusted hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path; and

the trusted hardware module is operable to use the response in generating an integrity metric of the apparatus.

9. (Previously Presented) An apparatus as claimed in claim 1, wherein:

the first further hardware module has a zone for private data and a zone for non-private data; and

the first further hardware module is operable to supply and/or receive data from/for the private data zone via the first communication path and not via the shared communication infrastructure.

10. (Previously Presented) An apparatus as claimed in claim 9, wherein the first further hardware module is operable to supply and/or receive data from/for the non-private data zone via the shared communication infrastructure.

11. (Previously Presented) An apparatus as claimed in claim 10, wherein the first further hardware module has an interface between the private and non-private data zones which is operable to inhibit the passing of data from the private data zone to the non-private data zone.

12. (Previously Presented) An apparatus as claimed in claim 1, wherein the first further hardware module is a network interface module.

13. (Previously Presented) An apparatus as claimed in claim 1, and including a second communication path, distinct from the shared communication infrastructure and the first communication path, by which a second one of the further hardware modules can communicate

directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

14. (Previously Presented) An apparatus as claimed in claim 13, wherein:

the first further hardware module is operable to supply to the trusted hardware module a request for a transfer of data between the first and second further hardware modules; and

in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first or second further hardware module via the first or second communication path, respectively, and not via the shared communication infrastructure.

15. (Previously Presented) An apparatus as claimed in claim 14, wherein the trusted hardware module includes means for storing policy information regarding such transfers which can or cannot be permitted, and is operable to generate the response with reference to the policy information.

16. (Currently Amended) An apparatus as claimed in claim 14, wherein:

in response to an appropriate such transfer response, the first or second further hardware module is operable to supply the data to the trusted hardware module via the first or second communication path, ~~as the case may be~~ respectively; and

in response to the receipt of such data, the trusted hardware module is operable to relay the data to the second or first further hardware module, respectively, via the second or first communication path, as the case may be.

17. (Previously Presented) An apparatus as claimed in claim 13, wherein the second further hardware module is a main processor unit of the apparatus or a non-volatile data storage module.

18. (Previously Presented) An apparatus as claimed in claim 13, and including at least a third communication path, distinct from the shared communication infrastructure and the other communication paths, by which at least a third one of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules.

19. (Previously Presented) An apparatus as claimed in claim 18, wherein the second further hardware module is a main processor unit of the apparatus and the third further hardware module is a non-volatile data storage module.

20. (Previously Presented) An apparatus as claimed in claim 1, wherein the trusted hardware module is adapted to measure an integrity metric of the computing apparatus.

21. (Previously Presented) A computing apparatus comprising:

a trusted hardware module resistant to unauthorized modification;

a plurality of further hardware modules;

a shared communication infrastructure by which the hardware modules can communicate with each other; and

a first communication path distinct from the shared communication infrastructure by which a first one of the further hardware modules can communicate directly with the trusted hardware module but which is inaccessible to the other further hardware modules.

22. (Previously Presented) An apparatus as claimed in claim 21, wherein the trusted hardware module and the first further hardware module each include a respective computing engine which partakes in the direct communication via the first communication path.

23. (Previously Presented) An apparatus as claimed in claim 22, wherein:

the first further hardware module is operable to supply to the trusted hardware module a request for operation on data; and

in response to such a request, the trusted hardware module is operable to generate a response and to supply the response to the first further hardware module via the first communication path and not via the shared communication infrastructure.

24. (Previously Presented) An apparatus as claimed in claim 23, wherein the trusted hardware module includes means for storing policy information regarding such operations which can or cannot be permitted, and is operable to generate the response with reference to the policy information.

25. (Previously Presented) An apparatus as claimed in claim 21, wherein the trusted hardware module is operable to generate an encryption and/or decryption key and to supply that key to the first further hardware module via the first communication path and not via the shared communication infrastructure.

26. (Previously Presented) An apparatus as claimed in claim 25, wherein the first further hardware module is operable to use the key for encryption and/or decryption of data communicated via the shared communication infrastructure.

27. (Previously Presented) An apparatus as claimed in claim 21, wherein the trusted hardware module is operable to generate a challenge and to supply the challenge to the first further hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path.

28. (Previously Presented) An apparatus as claimed in claim 27, wherein:

in response to the challenge, the first further hardware module is operable to generate a response and to supply the response to the trusted hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path; and

the trusted hardware module is operable to use the response in generating an integrity metric of the apparatus.

29. (Previously Presented) An apparatus as claimed in claim 21, wherein the first further hardware module is a network interface module.

30. (Previously Presented) An apparatus as claimed in claim 21, wherein the trusted hardware module is adapted to measure an integrity metric of the computing apparatus.